Implementing Cybersecurity Standards: Approaches to Securing Infrastructure through an Executive Framework

By Clark Taylor
LLNL Cyberdefenders Program

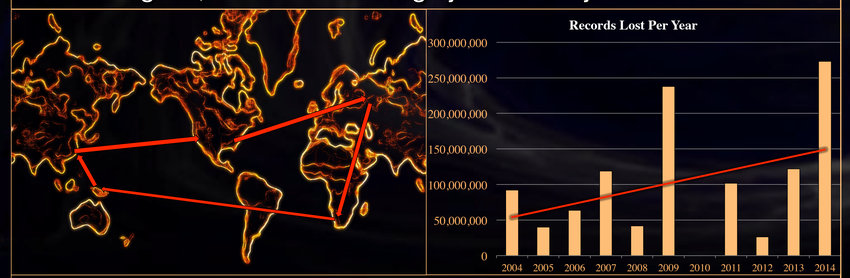
As technology progresses, digitizing and networking ever more systems, the ability of malicious actors to take advantage of those systems grows as well. However, cybersecurity measures have not kept up with the increasing threats and attacks resulting from the trend. This project examines legal and policy measures which could be taken in order to counter the cyber threat today. Ultimately, this project concludes that a proposed expansion of the NIST Cybersecurity Framework may provide the most advantageous response to these challenges.

Introduction:

- Digital, and particularly communications, technology continues its trend towards ever larger device integration, bolstering efficiency.
- However, this trend also presents new targets for malicious actors.
- Individuals, businesses, and even state actors may wish to take advantage of certain systems for a variety of different reasons:
  - Hactivism/personal political beliefs
  - Economic gain
  - International relations motivators/diplomatic reasons
- Attacks have increased with vulnerabilities.
- Estimates put annual losses due to attack at over $400,000,000,000
- As more systems become integrated, attacks may prove ever more damaging.

The Problem:

- Traditional legal approaches, such as criminalizing certain activities, tend to be ineffective against cyber crime for several reasons:
  - The internet does not readily identify those who commit crimes.
  - The international nature of the internet causes jurisdiction issues.
  - Technical developments and international agreements hold little promise in confronting these issues.
- Potential targets can, however, take measures to protect themselves.
- Strong standards, when properly implemented, tend to accomplish these goals.
- In some cases, businesses may strongly self regulate with regards to cyber security by creating standards organizations.
- Many other industries, notably critical infrastructure areas such as electric grids, do not have strong cyber security standards.



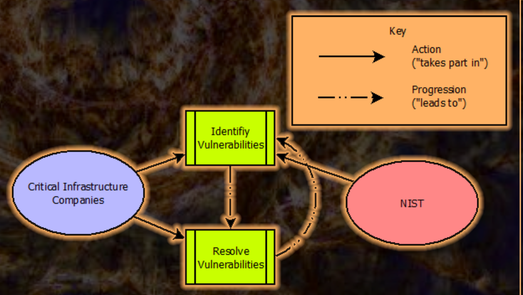
The chart on the right provides the sum of records lost in known attacks affecting more than 10 million records per year since 2004, while the map on the left illustrates how attacks may traverse international borders.

Executive Action:

- In order to confront the cybersecurity threats facing critical infrastructure, the President of the United States issued Executive Order 13636 and Presidential Policy Directive 21.
- Presidential Policy Directive 21 aimed to create general areas of responsibility regarding cybersecurity in critical infrastructure.
- Executive Order 13636 mandated the production of a federal cybersecurity framework wherein government agencies may work with critical infrastructure companies in order to counter cyber threats. The order made the National Institute of Standards and Technology responsible for the development of such a framework.
- After gathering information and considering the problem, the NIST developed and published their framework on February 14, 2014.

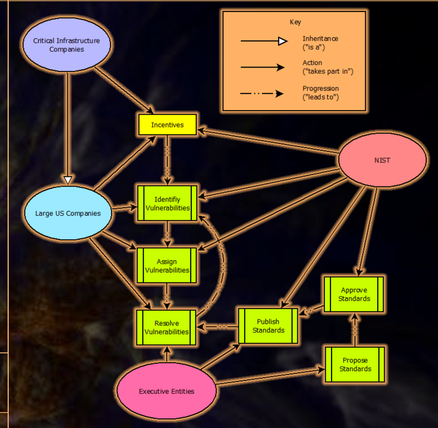
Current Framework:

The diagram on the right demonstrates the main points of the NIST framework, wherein that agency works with critical infrastructure companies to identify vulnerabilities.



- The first and current iteration of the NIST framework has three main steps:
  - A critical infrastructure operator or owner comes to the NIST and voluntarily participates in the framework.
  - NIST works with the company to identify their ideal level of security, then pinpoints crucial vulnerability categories in that company's systems; NIST also offers some level of guidance regarding how the company may achieve its ideal level of security.
  - The company, on its own accord and without government involvement, attempts to fix the identified vulnerabilities. After that, the company may return to NIST and begin again.
- The NIST Framework presents a strong step in the right direction.

Proposed Framework:



The diagram on the left illustrates the executive cybersecurity framework proposed here. In it, the NIST first provides incentives to coax businesses into participation. After that, NIST identifies vulnerabilities and passes them to other agencies to resolve with the participating companies. Separately, executive agencies may propose and implement standards for certain areas to be used in resolving the fore mentioned vulnerabilities.

Potential incentives:

- Direct federal participation requirement
- Government program/contract terms
- State law preemption
- Tax breaks
- Grant funding
- Quality of the framework
- Liability adjustment

- The NIST Framework takes the most effective approach towards cybersecurity by implementing a federal framework aimed at helping businesses deal with vulnerabilities.
- However, the NIST Framework falls short due to several issues:
  - While NIST produces standards in numerous areas, it does not have the technical competency to deal with the variety of infrastructure companies may bring to the Framework.
  - The NIST approach does not take advantage of standardized solutions to common problems which can be quite effective.
  - The NIST Framework approaches vulnerabilities from the top down, which can miss important details in the systems.
  - NIST has not yet dealt with how to properly incentivize their framework, relying on voluntary participation only at this point. This is likely not enough incentive to have companies enter the Framework.
- In order to deal with these flaws, this project recommends the following changes to the NIST Framework:
  - Assign vulnerabilities to appropriate executive agencies which then collaborate with businesses to find resolutions.
  - Allow executive agencies to propose and implement solutions, which NIST then reviews, approves, and compiles in a cyber security standards repository available to Framework users.
  - Provide proper incentives, managed by NIST when appropriate, for companies to enter the framework, such as those listed above.

This work performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under Contract DE-AC52-07NA27344.

LLNL-POST-658244